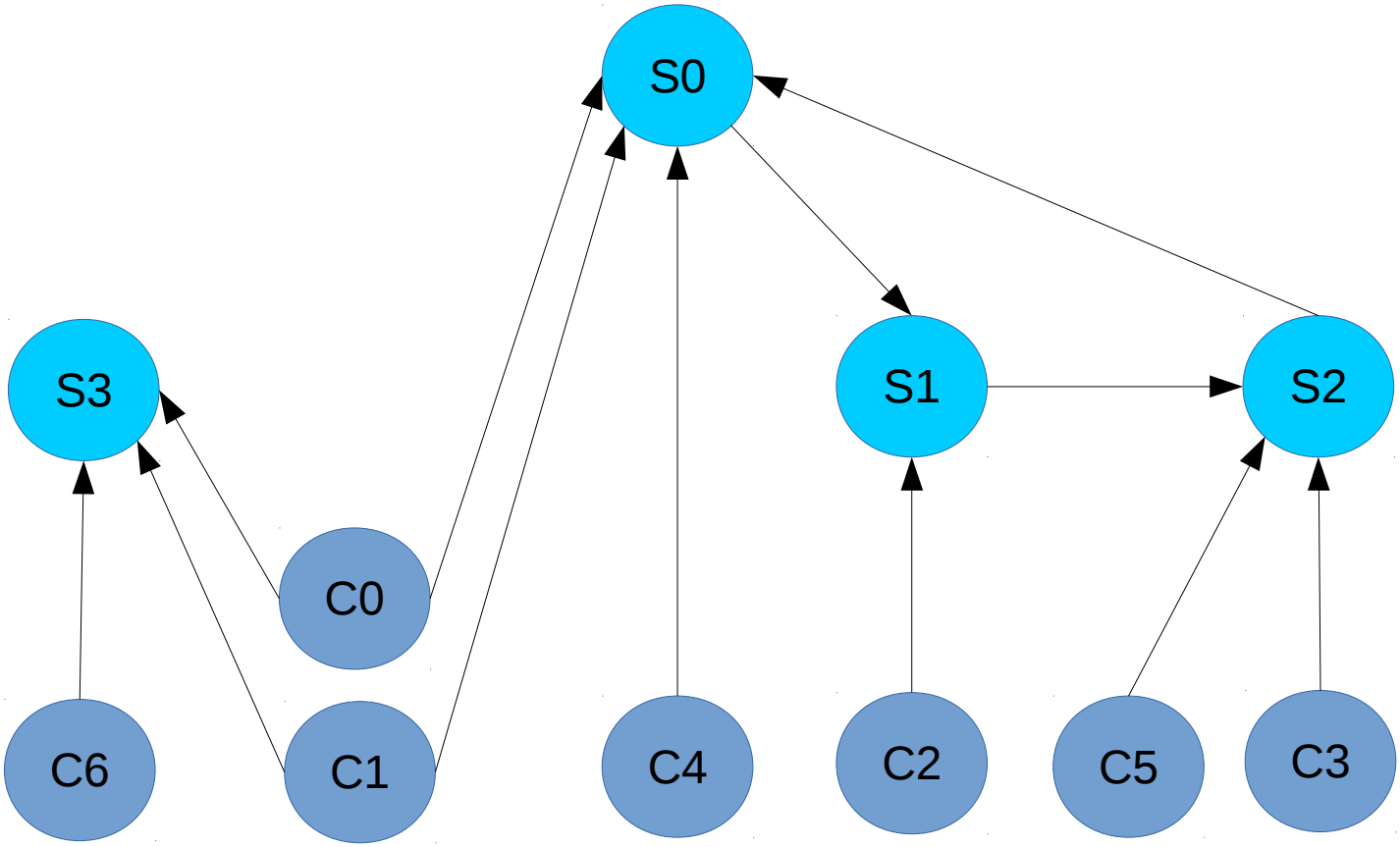
Cryptographic Discovery on the Echo Protocol (CDE)



Cryptographic Discovery on the Echo Protocol (CDE)

Let's explain the Cryptographic Discovery on the Echo Protocol (CDE) through a simple example.

We'll describe several details and the remaining should become self-explanatory. In its brief form, Cryptographic Discovery is a simple protocol where clients share presence information with nearby servers. Nearby servers, if acting as clients, share their information with nearby servers, and so on. Presence information is shared whenever necessary.

In the above diagram, the Cs represent clients whereas the Ss represent servers. Servers may behave as clients (see directions of arrows).

Let C4 and S0 establish a network connection. The connection need not support SSL/TLS. Assuming that a correct connection has been established, C4 will optionally share some non-private discovery details with S0. This information may include, e.g., digests of Buzz magnets, digests of StarBeam magnets, digests of personal public keys, etc. Some of this information may also be shared later. Also suppose that C1 performs a similar task.

As the network contracts and expands, entities such as S0 become aware of some of the virtual addresses of C0, C1, C4, and S2.

- Notice that S0 is not aware of neither C6 nor S3 because the paths to S3 are inward.
- Also notice that S0 may become aware of C3 and C5 courtesy of S2.

What's the purpose of Cryptographic Discovery? CDE's primary purpose is to place the burden of data inspection on certain servers.
Servers will be able to direct traffic by inspecting packets and delivering them to their correct clients.

Let's assume that the above network is static for the remaining portion of the exercise. Let's also assume that the discovery process has established sufficient knowledge with each of the servers.

Now, suppose C4 wishes to communicate with C3. C4 will deliver a message to S0. S0, having a delicate knowledge database, will deliver the message to S2. Likewise, S2 will deliver the message to C3. Without Cryptographic Discovery, C4's message would spread through the entire network over the Echo Protocol.